# IQRF® Communication Standard

for wireless mesh networks

IQRF Reliable by definition™

Specification can be changed without notice

## Abstract

Since 2004, MICRORISC s.r.o. and IQRF Tech s.r.o. have developed a low-cost, low-power, two-way, wireless mesh communication technology. Thanks to the 2-decades continuous development for and with our customers, we created state-of-art communication technology for wireless mesh networks featuring values:

- Industrial reliability,
- simple integration,
- ultimate security,
- interoperability and huge ecosystem,
- true low power efficiency.

Dozens of patents were granted, protecting the IQRF® and its implementors from plagiarism and saving their investments.

The IQRF® moves to the third decade as an open standard. This document discloses the specifications needed for the IQRF standard implementation. The IQRF standard implementations and use of all IQRF standard-related essential patents are allowed under a single royalty-free license.

## Keywords

Wireless; Mesh; Networks; IQRF; Standard; Open; Free

## Patents and licensing

Specific protocols, arrangements, and solutions described in this specification are protected by one or more patents in Czech, EU, USA, China, and Japan. A single royalty-free license allows the IQRF standard implementation and use of all IQRF Standard related essential patents. For details, check the website https://standard.iqrf.org.

## Copyright



IQRF Standards Association z.s.
Prumyslova 1275
506 01 Jicin
Czech Republic, EU

Quick link to Table of contents



# 1. DOCUMENT

## 1.1. HISTORY AND REVISIONS

| revision | date | description |
|---|---|---|
| 230807 | August 07, 2023 | preliminary documentation draft |
| 231117 | November 17, 2023 | The EAP release under NDA only, v ICSS 0.91 |
| 240303 | March 03, 2024 | The public release, ICSS v 0.95 |
| 240331 | March 31, 2024 | The public release, ICSS v 0.96 |

## 1.2. AUTHORS AND CHAPTERS SUPERVISORS

- General concept and the first public release of the Specification
  - Vladimír Šulc, Ph.D., MICRORISC s.r.o.,
- Chapter 10 Security specification:
  - Ondřej Hujňák, Brno Technical University, Faculty of Informatics,
- Annex A – Region related setup:
  - Pavel Plecháč, Jiří Poš, MICRORISC s.r.o.,
- Special thanks to:
  - MICRORISC R&D team for the continual support and the IQRF legacy implementations,
- Acknowledgements:
  - Ministry of Industry and Trade of Czech Republic for the financial support of IQRF-related projects,
  - The Brno University of Technology, Faculty of Electrical Engineering and Communication, for cooperation in IQRF-related projects,
  - The Technical University of Ostrava, Faculty of Electrical Engineering and Computer Science, for cooperation in IQRF-related projects.

## 1.3. SCOPE

This document contains specifications and descriptions of processes, data structures, security, interfaces, protocols, timings, and algorithms related to the IQRF standard.

## 1.4. PURPOSE

The purpose of this document is to provide a complete description of the IQRF standard as a basis for implementing interoperable, low-cost, highly reliable, and usable products for wireless mesh applications. Implementations of the IQRF standard shall keep definitions and rules described in this specification, especially data structures, process flows, and timings, to ensure devices interoperability**.** Implementations, on the other hand, should be optimized for the ported MCUs and radios.

## 1.5. DESIGN ARCHITECTURE

The IQRF layered architecture design is based on the ISO OSI standard recommendations. Each layer performs a specific set of services for the layer above. Detailed architecture is depicted in Figure 1.



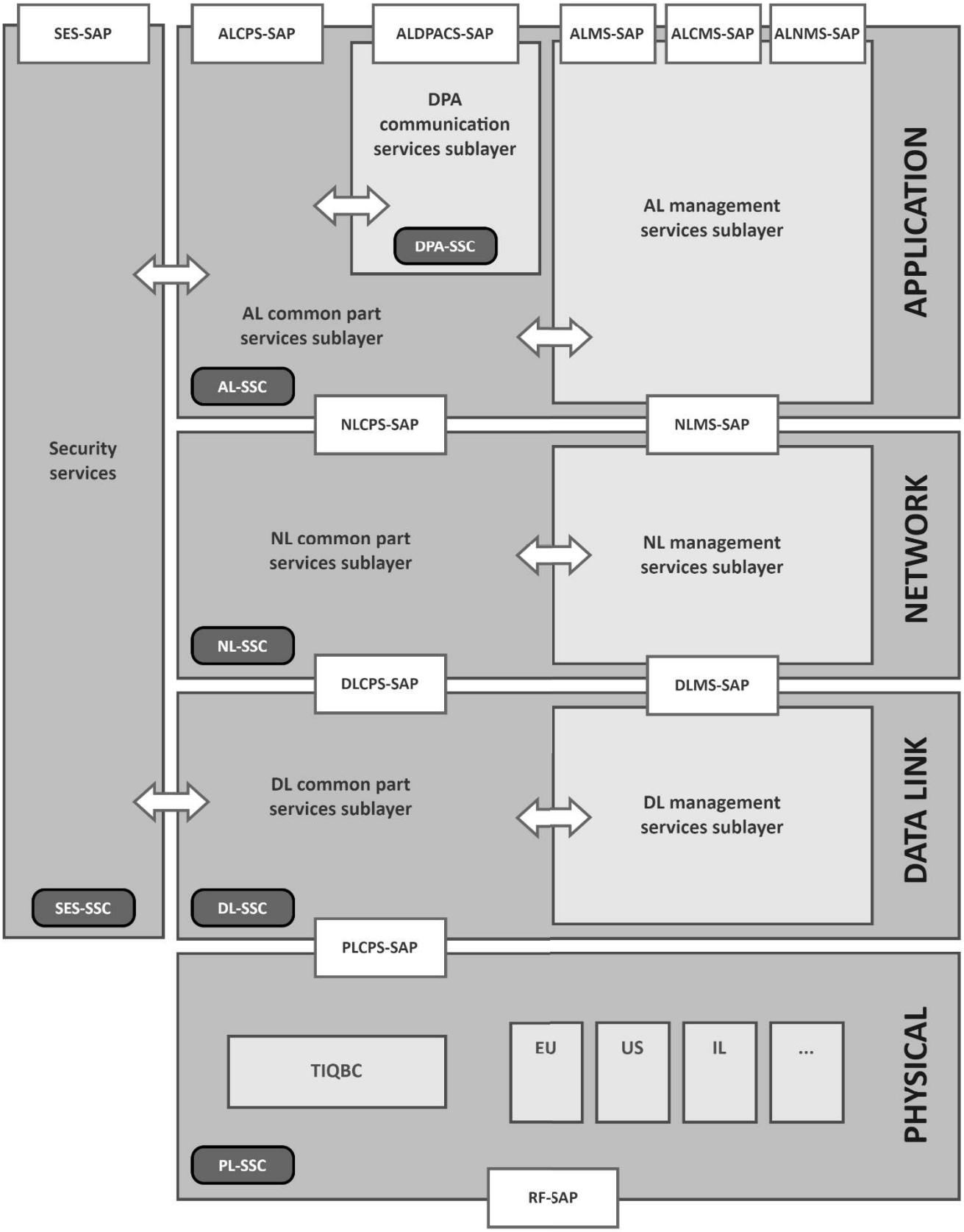



Figure 1: IQRF standard design architecture



## 1.6. ACRONYMS

| | |
|---|---|
| AES | Advanced encryption standard |
| AL | Application layer |
| ALCMS-SAP | ALMS service access point (coordinator) |
| ALCPS | Application layer common part services (sublayer) |
| ALDPACS | Application layer DPA communication services (sublayer) |
| ALMS | Application layer management services |
| ALNMS-SAP | ALMS service access point (node) |
| AL-SSC | Application Layer System Setup and Configuration |
| ASID | Association ID |
| ASPS | Association PHY setup |
| BED | Beaming device (device class) |
| BEN | Beaming node |
| BNCK | Base Network Communication Key |
| CBC | Cipher Block Chaining |
| CBC-MAC | Cipher block chaining message authentication code |
| CCM | Counter with CBC-MAC |
| CRC | Cyclic redundancy check |
| CSMA | Carrier sense multiple access |
| CSMA-CA | Carrier sense multiple access with collision avoidance |
| DFR | Data link footer |
| DHR | Data link header |
| DJK | Device joining key |
| DL | Data Link or Data Link Layer |
| DLCPS | Data Link Common Part Services (sublayer) |
| DLK | Data link key |
| DLMS | Data Link Management Services (sublayer) |
| DL-SSC | System Setup and Configuration for Data link Layer |
| DPA | Direct Peripheral Access |
| F-ASA | ASSOCIATED frame for active association |
| F-ASP | ASSOCIATED frame for passive association |
| FCE | Frame Control Element |
| FCS | Frame control setup |
| F-JR | JOIN-REQUEST frame |
| FNF | Fixed network frame |
| FRC | Fast response command |
| FRE | Frame element |
| FRXE | SSC FRX element |
| FSK | Frequency shift keying |
| FTXE | SSC FTX element |
| GFSK | Gaussian frequency-shift keying |
| ICS | IQRF communication standard |

| | |
|---|---|
| ICSS | IQRF communication standard specification |
| IMAC | IQRF MAC address |
| IQRF-SA | IQRF Standards Association |
| IUK | Individual unicast key |
| IWMN | IQRF wireless mesh network |
| KDF | Key derivation function |
| LBT | Listen before talk |
| LPLN | Low power and lossy network |
| LPRX | Low power receive (mode) |
| LPTX | Low power transmission (mode) |
| LSb | Least significant bit |
| LSB | Least significant byte |
| MAC | Message authentication code |
| MAC | Medium access control |
| MSb | Most significant bit |
| MSB | Most significant byte |
| NAK | Network access key |
| NHL | Next higher layer |
| NHLE | Next Higher Layer Entity |
| NHR | Network header |
| NID | Network identification |
| NL | Network layer |
| NLCPS | Network layer common part services |
| NLL | Next Lower Layer |
| NLMS | Network layer management services |
| NL-SSC | Network layer system setup and configuration |
| NRN | Non-routing node |
| OFMO | Offline mode |
| PDU | Protocol data unit |
| PFR | PHY footer |
| PHR | PHY header |
| PHY | Physical or PHY (layer) |
| PL | PHY layer |
| PLCPS | Physical link layer common part services |
| PL-SSC | Physical layer system setup and configuration |
| PNPS | Particular network PHY setup |
| PPS | Primitive parameters setup |
| RF | Radio frequency |
| RFIC | Radio frequency integrated circuit |
| RIDX | Rotation index |
| RON | Routing node |
| RON/A | RON or RONA |
| RONA | Routing node with aggregation |

| | |
|---|---|
| ROR | Router (device class) |
| ROR/A | ROR or RORA |
| RORA | Aggregating router (device class) |
| RRPS | Region related PHY setup |
| RSSI | Received signal strength indication |
| RTHR | Routing header |
| RX | Receive or Receiver |
| RXMO | Online mode |
| SAP | Service access point |
| SES | Security services (layer/block) |
| SES-SSC | SES system setup and configuration |
| SNF | Standard network frame (no routing support) |
| SNFR | Standard network frame (supporting routing) |
| SNNF | Standard non-network frame |
| SSC | System setup and configuration |
| SSCE | SSC element |
| SSC-FRX | SSCE Frame RX |
| SSC-FTX | SSCE Frame TX |
| SSCID | SSC element ID |
| STDRX | Standard receive (mode) |
| STDTX | Standard transmission (mode) |
| TDMA | Time division multiple access |
| TICSS | This IQRF communication standard specification |
| TIQBC | Time quanta bit coding |
| TLL | Time-Limited loop |
| TX | Transmit or Transceiver |
| VRN | Virtual routing number |
| WMN | Wireless mesh network |
| XLPTX | Extra low power transmission (mode) |

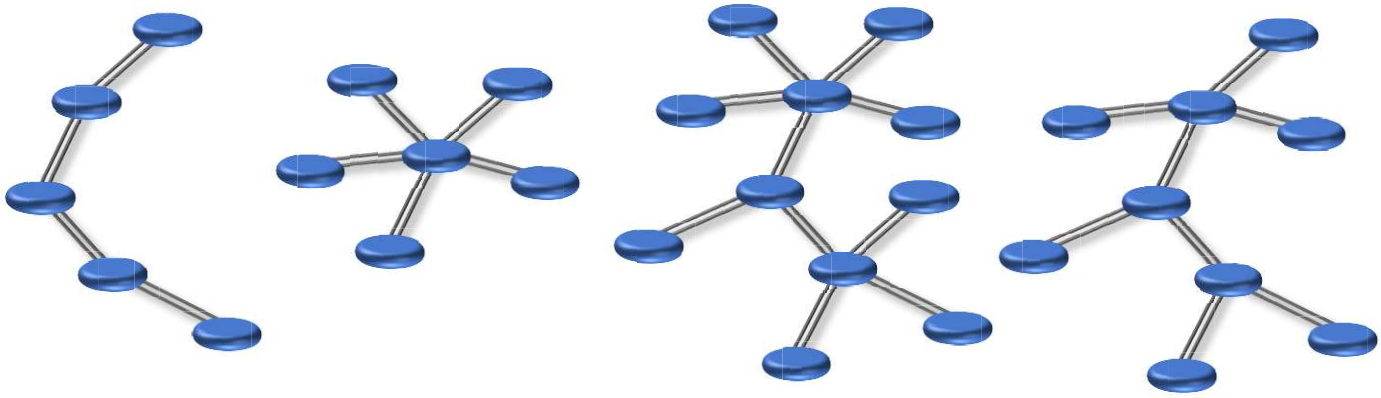
1

# 4. IQRF BRIEF OVERVIEW

Only fundamental principles are described here. A detailed functional description is available in Chapter 11.

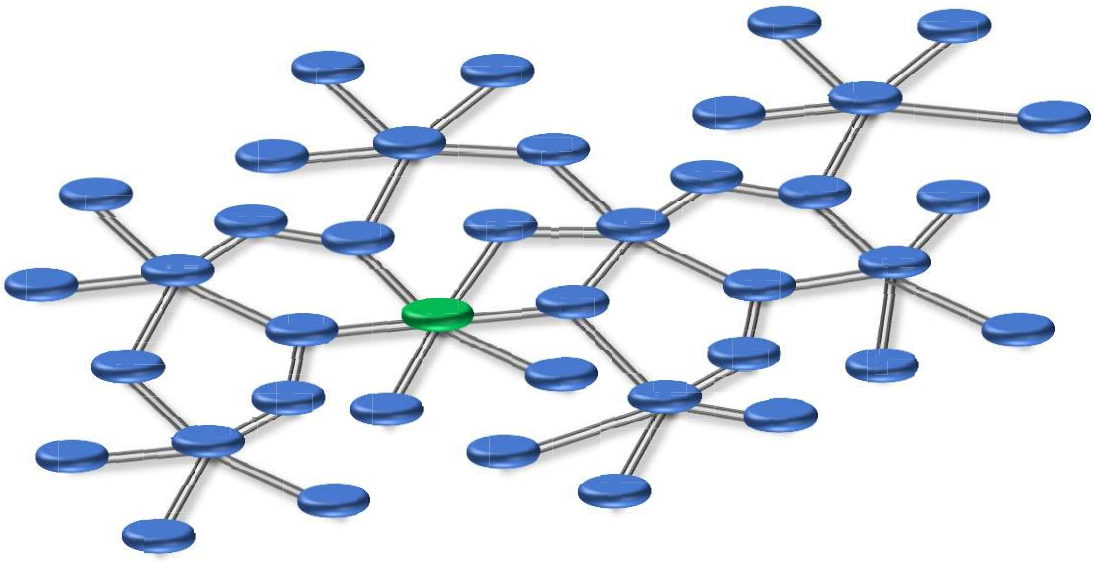
## 4.1. GENERAL WIRELESS MESH NETWORKS

Wireless mesh networks are a type of network setup that involves multiple wireless router nodes or points spreading across a large area to provide Internet or network coverage. Unlike traditional networks, which rely on a small number of wired access points or wireless routers, mesh networks consist of many wireless nodes that communicate with each other to spread the network coverage over a vast area. This setup allows data to be relayed across the nodes, finding the fastest and most efficient path to its destination. Mesh network topology is the most general network arrangement, including many other distinguished topologies, like the chain, star, or tree. Examples of mesh networks are depicted in the figure below.



## 4.2. IQRF MESH NETWORK

IQRF networks are organized and orchestrated. The coordinator is such a conductor for other network devices called nodes. Nodes with the routing capability are called routers. The network communication is always encrypted and authenticated according to the latest security standards. The IQRF networks support up to 1024 devices and up to 255 routing hops. Typical IQRF network arrangement is depicted in figure below.



## 4.3. NETWORK DEVICES

### 4.3.1. COORDINATOR

Coordinator is a device orchestrating the IQRF network and associating other devices, nodes, to the network. Network address of the coordinator and its Virtual routing number are always 0x00.

### 4.3.2. NODE

Node is a general device joining the IQRF network.

#### 4.3.2.1. ROUTING NODE

Routing nodes are nodes associated to the network with addresses 1 – 255. Routing nodes participate in the routing and in the aggregation phase of the FRC protocol.

#### 4.3.2.2. ROUTING NODE WITH THE AGGREGATION

Routing nodes with aggregation are routing nodes with the capability of listening to the beaming nodes, store their transmissions and provide requested data from these transmissions through the FRC protocol.

#### 4.3.2.3. NON-ROUTING NODE

Non-routing nodes are node devices associated to the network with addresses 256 – 511. Non-routing nodes are always in receiving and processing incoming transmissions, they do not participate in the routing.

#### 4.3.2.4. BEAMING NODE

Beaming node is a low power node associated to the network with addresses 512 – 1023. Beaming nodes awake periodically or upon defined conditions to transmit their data. Beaming nodes do not participate in the routing and due to the minimizing consumption are not responding to the standard network communication unless they do not switch to the receive mode.

## 4.4. CREATING THE NETWORK

### 4.4.1. ASSOCIATION OF JOINING DEVICES

The association is the process controlled by the coordinator and used to establish membership in a network for joining nodes. The coordinator shares bonding information, such as communication keys and network setup, with nodes in a secure way through the encrypted payload and dedicates a unique network address to each node. The IQRF MAC address is used for authentication as a unique identifier of IQRF devices.

### 4.4.2. DISCOVERY OF ROUTING DEVICES TOPOLOGY

The discovery is the process by which the coordinator discovers routing nodes' topology and dedicates them the Virtual Routing Number, a unique number reflecting distance from the coordinator in hops and defining a time slot during routing.

## 4.5. NETWORK COMMUNICATION

In most application scenarios, the coordinator initiates communication, and nodes respond through the IQMESH and FRC protocols. Routed networking communication is always orchestrated while beaming nodes transmit their data asynchronously.



### 4.5.1. DATA AND SYSTEM COMMUNICATION

There are two basic types of communication – data communication and system communication.

Data communication is realized through the standard data frames and enables data delivery to the next higher layer above the application layer.

The system communication supports protocols and functionality described in the IQRF standard specification; the application and lower layers process it, and data are not provided to the layers above the application layer. The system communication is realized through standard non-network, standard networking, and fixed network frames.

### 4.5.2. COMMUNICATION SECURITY

System non-networking and complete networking communication is always encrypted and authenticated as described in this specification.

## 4.6. ADDRESSING

The IQRF supports the following addressing modes without acknowledgment

- Unicast from the coordinator to any node,
- unicast from the routing node to the coordinator,
- broadcast sent by the coordinator to all network devices,
- broadcast sent by the coordinator or by the node to the neighboring devices.

The IQRF supports the following acknowledged addressing modes:

- Broadcast initiated by the coordinator (FRC protocol),
- multicast initiated by the coordinator (FRC protocol),
- selectivecast initiated by the coordinator (FRC protocol),
- broadcast initiated by the node (local FRC protocol),
- selectivecast initiated by the node (local FRC protocol).

## 4.7. IQMESH® ROUTING PROTOCOL

IQMESH routing protocol is collision-free, based on the TDMA and oriented flooding, supporting unicast, broadcast, groupcast, and selectivecast. It is deterministic and reliable and perfectly works even under challenging environments.

The coordinator detects routing nodes topology during the discovery. Based on the discovered topology the coordinator dedicates the Virtual Routing Number to routing nodes. The virtual routing number is a unique number reflecting distance from the coordinator in hops and defining a time slot during routing. Thanks to the virtual routing number each router knows its position in the network and its dedicated time slot.

TDMA and VRN-based directional flooding guarantees deterministic and collision-free routing.

## 4.8. FRC® DATA AGGREGATION PROTOCOL

The FRC protocol is based on the IQMESH network arrangements and routing protocol. It enables fast data aggregation and acknowledged broadcasts/multicasts. The FRC protocol further increases IQMESH protocol reliability and provides high-level robustness and successful delivery even under very challenging conditions, being an excellent solution for lossy, low-rate wireless mesh networks.

The FRC protocol supports acknowledged broadcast and multicast, and thanks to its high efficiency and reliability, it is an excellent tool for network management.

## 4.9. IQRF DPA PROTOCOL

Direct Peripheral Access (DPA) protocol is a simple byte-oriented protocol used to control services and peripherals of the IQRF network devices directly from device interfaces such as SPI or UART. IQRF standard specification defines only data communication service support via the DPA protocol. A complete description of the IQRF DPA protocol is available at https://iqrf.org/dpa.

## 4.10. IQRF SECURITY

The Security Services layer is responsible for ensuring the following security objectives:

- Frame integrity
- Networking frame authenticity
- Footer and Payload confidentiality
- Replay protection

The IQRF uses authenticated encryption with associated data (AEAD) based on the NIST standardized CCM scheme.

# 17. LIST OF FIGURES





# 18. TABLE OF CONTENTS